(b) If the third-party auditor or certification organization has found that a pharmacy application does not accurately and consistently import, store, and display other information required for prescriptions under this chapter, the pharmacy must not process electronic prescriptions for controlled substances that are subject to the additional information requirements.

(c) If a pharmacy application provider notifies a pharmacy that a third-party audit or certification report indicates that the application or the application provider no longer meets the requirements of this part or notifies it that the application provider has identified an issue that makes the application non-compliant, the pharmacy must immediately cease to process controlled substance prescriptions using the application.

(d) A pharmacy that receives a notification that the pharmacy application is not in compliance with the requirements of this part must not use the application to process controlled substance prescriptions until it is notified that the application is again compliant and all relevant updates to the application have been installed.

(e) The pharmacy must determine which employees are authorized to enter information regarding the dispensing of controlled substance prescriptions and annotate or alter records of these prescriptions (to the extent such alterations are permitted under this chapter). The pharmacy must ensure that logical access controls in the pharmacy application are set so that only such employees are granted access to perform these functions.

(f) When a pharmacist fills a prescription in a manner that would require, under part 1306 of this chapter, the pharmacist to make a notation on the prescription if the prescription were a paper prescription, the pharmacist must make the same notation electronically when filling an electronic prescription and retain the annotation electronically in the prescription record or in linked files. When a prescription is received electronically, the prescription and all required annotations must be retained electronically.

(g) When a pharmacist receives a paper or oral prescription that indicates that it was originally transmitted electronically to the pharmacy, the pharmacist must check its records to ensure that the electronic version was not received and the prescription dispensed. If both prescriptions were received, the pharmacist must mark one as void.

(h) When a pharmacist receives a paper or oral prescription that indicates that it was originally transmitted electronically to another pharmacy, the pharmacist must check with that pharmacy to determine whether the prescription was received and dispensed. If the pharmacy that received the original electronic prescription had not dispensed the prescription, that pharmacy must mark the electronic version as void or canceled. If the pharmacy that received the original electronic prescription dispensed the prescription, the pharmacy with the paper version must not dispense the paper prescription and must mark the prescription as void.

(i) Nothing in this part relieves a pharmacy and pharmacist of the responsibility to dispense controlled substances only pursuant to a prescription issued for a legitimate medical purpose by a practitioner acting in the usual course of professional practice.

§ 1311.205 Pharmacy application requirements.

(a) The pharmacy may only use a pharmacy application that meets the requirements in paragraph (b) of this section to process electronic controlled substance prescriptions.

(b) The pharmacy application must meet the following requirements:

(1) The pharmacy application must be capable of setting logical access controls to limit access for the following functions:

(i) Annotation, alteration, or deletion of prescription information.

(ii) Setting and changing the logical access controls.

(2) Logical access controls must be set by individual user name or role.

(3) The pharmacy application must digitally sign and archive a prescription on receipt or be capable of receiving and archiving a digitally signed record.

(4) For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality must meet the following requirements:

(i) The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter must be at least FIPS 140–2 Security Level 1 validated. FIPS 140–2 is incorporated by reference in §1311.08.

(ii) The digital signature application and hash function must comply with FIPS 186–3 and FIPS 180–3, as incorporated by reference in §1311.08.

(iii) The pharmacy application's private key must be stored encrypted on a FIPS 140–2 Security Level 1 or higher validated cryptographic module using a FIPS-approved encryption algorithm. FIPS 140–2 is incorporated by reference in §1311.08.

(iv) For software implementations, when the signing module is deactivated, the pharmacy application must clear the plain text password from the application memory to prevent the unauthorized access to, or use of, the private key.

(v) The pharmacy application must have a time application that is within five minutes of the official National Institute of Standards and Technology time source.

(5) The pharmacy application must verify a practitioner's digital signature (if the pharmacy application accepts prescriptions that were digitally signed with an individual practitioner's private key and transmitted with the digital signature).

(6) If the prescription received by the pharmacy application has not been digitally signed by the practitioner and transmitted with the digital signature, the pharmacy application must either:

(i) Verify that the practitioner signed the prescription by checking the data field that indicates the prescription was signed; or

(ii) Display the field for the pharmacist's verification.

(7) The pharmacy application must read and retain the full DEA number including the specific internal code number assigned to individual practitioners authorized to prescribe controlled substances by the hospital or other institution as provided in §1301.22(c) of this chapter.

(8) The pharmacy application must read and store, and be capable of displaying, all information required by part 1306 of this chapter.

(9) The pharmacy application must read and store in full the information required under §1306.05(a) of this chapter. The pharmacy application must either verify that such information is present or must display the information for the pharmacist's verification.

(10) The pharmacy application must provide for the following information to be added or linked to each electronic controlled substance prescription record for each dispensing:

(i) Number of units or volume of drug dispensed.

(ii) Date dispensed.

(iii) Name or initials of the person who dispensed the prescription.

(11) The pharmacy application must be capable of retrieving controlled substance prescriptions by practitioner name, patient name, drug name, and date dispensed.

(12) The pharmacy application must allow downloading of prescription data into a database or spreadsheet that is readable and sortable.

(13) The pharmacy application must maintain an audit trail of all actions related to the following:

(i) The receipt, annotation, alteration, or deletion of a controlled substance prescription.

(ii) Any setting or changing of logical access control permissions related to the dispensing of controlled substance prescriptions.

(iii) Auditable events as specified in §1311.215.

(14) The pharmacy application must record within each audit record the following information:

(i) The date and time of the event.

(ii) The type of event.

(iii) The identity of the person taking the action, where applicable.

(iv) The outcome of the event (success or failure).

(15) The pharmacy application must conduct internal audits and generate

reports on any of the events specified in §1311.215 in a format that is readable by the pharmacist. Such an internal audit may be automated and need not require human intervention to be conducted.

(16) The pharmacy application must protect the stored audit records from unauthorized deletion. The pharmacy application shall prevent modifications to the audit records.

(17) The pharmacy application must back up the controlled substance prescription records daily.

(18) The pharmacy application must retain all archived records electronically for at least two years from the date of their receipt or creation and comply with all other requirements of §1311.305.

§1311.210 Archiving the initial record.

(a) Except as provided in paragraph (c) of this section, a copy of each electronic controlled substance prescription record that a pharmacy receives must be digitally signed by one of the following:

(1) The last intermediary transmitting the record to the pharmacy must digitally sign the prescription immediately prior to transmission to the pharmacy.

(2) The first pharmacy application that receives the electronic prescription must digitally sign the prescription immediately on receipt.

(b) If the last intermediary digitally signs the record, it must forward the digitally signed copy to the pharmacy.

(c) If a pharmacy receives a digitally signed prescription that includes the individual practitioner's digital signature, the pharmacy application must do the following:

(1) Verify the digital signature as provided in FIPS 186–3, as incorporated by reference in §1311.08.

(2) Check the validity of the certificate holder's digital certificate by checking the certificate revocation list. The pharmacy may cache the CRL until it expires.

(3) Archive the digitally signed record. The pharmacy record must retain an indication that the prescription was verified upon receipt. No additional digital signature is required.

§1311.215 Internal audit trail.

(a) The pharmacy application provider must establish and implement a list of auditable events. The auditable events must, at a minimum, include the following:

(1) Attempted unauthorized access to the pharmacy application, or successful unauthorized access to the pharmacy application where the determination of such is feasible.

(2) Attempted or successful unauthorized modification or destruction of any information or records required by this part, or successful unauthorized modification or destruction of any information or records required by this part where the determination of such is feasible.

(3) Interference with application operations of the pharmacy application.

(4) Any setting of or change to logical access controls related to the dispensing of controlled substance prescriptions.

(5) Attempted or successful interference with audit trail functions.

(6) For application service providers, attempted or successful annotation, alteration, or destruction of controlled substance prescriptions or logical access controls related to controlled substance prescriptions by any agent or employee of the application service provider.

(b) The pharmacy application must analyze the audit trail at least once every calendar day and generate an incident report that identifies each auditable event.

(c) The pharmacy must determine whether any identified auditable event represents a security incident that compromised or could have compromised the integrity of the prescription records. Any such incidents must be reported to the pharmacy application service provider, if applicable, and the Administration within one business day.

§1311.300 Application provider requirements—Third-party audits or certifications.

(a) Except as provided in paragraph (e) of this section, the application provider of an electronic prescription application or a pharmacy application must have a third-party audit of the